ATTORNEY DOCKET NO.: 111325-81 (250100)

Application No.: 09/468,747

Page 2

Amendments to the Specification:

Page 36, lines 3-8, please amend, as follows:

The second observation is that, if the grantor A is the one who encrypts the message m, then A can keep the random number k private and use B's public key $\beta = g^b \pmod{p}$, instead of B's private key b, to generate the proxy key:

$$\pi = (\beta e \underline{a}^{-1})^k (\text{mod } p),$$

where α <u>a</u> is A's <u>public</u> <u>private</u> key. This eliminates the requirement for B's private key b (or key exchange between A and B), and implies that B does not have to trust A, either.